The frequency conundrum: modelling terrorism for the insurance industry

Mr Stephen Johnson, Research Fellow,
Cranfield Forensic Insttute

Summary

Many groups face the challenge of trying to make evidence based decisions about threats such as terrorism. Resource allocation by countries for security and resilience measures are a well-known challenge. While many countries keep this information extremely secret the USA has had its own methods reviewed publically by a number of respected bodies, such as the National Academy of Sciences. As recently as 2010 these reviews have been pretty negative in their conclusions (National Research Council, 2010). The UK and the Netherlands have also had their own national risk register processes reviewed in the open literature. Commensurate with some of the major national resource allocation challenges; the insurance industry has also faced a need to understand the frequency and impact of terrorism. While some catastrophic terrorism models exist in the market it has been regularly asserted that government backstopping is required because of a number of challenges in terrorism. Data sets are frequently included in this.

Aim

The unifying aim of this paper is that existing quantitative data can better forecast terrorist activity and inform resource allocation if structured correctly. Over reliance on elicitation techniques and probability trees open assessments to a variety of heuristics errors and biases. A stronger quantitative model would anchor assessments reducing these errors. This in turn would allow greater effectiveness in fighting terrorism and in the approach to assessing the relative merits of countermeasures. Before this improved approach is viable though some initial hypotheses must be tested:

Hypothesis 1 (H1): Terrorism data either does not exist, or is of poor quality for making forecasts.

Hypothesis 2 (H2): It is not feasible to make forecasts on the basis of this data, with confidence intervals and understanding of error margins.

Method

In order to fulfil this requirement the main open source databases of historical terrorist incidents were examined and compared. Particular focus was given to the presence or absence of code book, taxonomy, time period covered and collection methodology. Based on this, a period of time was defined for which the most databases had coverage in order to compare their records of terrorism. This cross comparison was focused on UK data due to the UK's clear, and public, counter terrorism strategy & national assessment. In further studies it may be useful to compare parts of the US with the UK systems because they also have publically available counter terrorism policies (DHS, 2007) (HMG, 2009) (HMG, 2006).

The databases used for this initial pilot were:

RAND Terrorism database (RTD). A think tank funded and administered database of terrorism incidents.

Global Terror Database (GTD). An amalgamation of the records of the Pinkerton agency terrorism database which was purchased by the University of Maryland, and 21 other separate projects. DHS funding has paid for its creation by merging all the sources and its purpose was to create a better database from which to start empirical analysis of terrorism.

Department of Homeland Security (DHS) Worldwide Incident Tracker (WIT). A US Government resource that tracks current and near/medium past incidents.

Monterey database of WMD incidents. An academic private access resource that tracks current and over 100 years history of CBRN incidents, plots and hoaxes.

Europol Terrorism Situation and trend report. As the name suggest and annual report produced on the trends of terrorism in the EU, alongside figures for counter terrorism activity in order to show the efficacy of certain measures.

These were selected as being the largest part processed (i.e. not raw press or reporting data) databases. There are other sources available specialized to types of attack and regions or groups. These will be reviewed in the creation of an improved model in later phases of the study.

Forecasting terrorism

The best data source available was identified using the analysis of the data sources. This was then imported in to a standalone database in order to allow manipulation and statistical analysis.

Step 1: A new database was created for each geographical region being studied

Step 2: A query was run to select only the dates for the selected time period.

Step 3: A further query generated 3 more data sets for each region:

- All incidents
- Incidents that killed at least 1 person
- Incidents that killed more than one person

Step 4: An analysis was carried out on each data set to assess its suitability for forecasting. This included autoregressive models and moving averages and move stationary and non-stationary time series analysis. Some models were optimised using the data set, others such as the moving averages were limited to only being able to predict after a number of years. Only the optimum models are included in this paper for brevity – these being the 3 and 6 year moving averages.

Comparison of terrorism databases

The fig 1 below of the number of recorded actual attacks by the five general terrorism databases shows the variation in data across the same time period in the databases for the UK. Fig 2 shows a comparison of the databases by attributes. The GTD and RAND low results are due to a tailing off in efforts recording incidents since 2007 when they were at their peak funding point, which has recently reversed for the GTD. Variation is on the whole down to the definition of terrorism used (or not) as the high level of media coverage of even the smaller attacks in Northern Ireland lend itself to being one of the simpler challenges in terrorism databases. The global terrorism database stands alone from all others as appearing to be the most inclusive dataset, but even it suffers from a legacy of synthesis from multiple databases pre-dating it. The Europol technique of allowing each country to set its own definition was a clever solution to the definition of terrorism challenge, but it equally highlighted huge differences between the number of attacks a country feels it has suffered and external observers opinions. It recorded for France many times more attacks than any other database – predominantly due to attacks on holiday homes in Corsica considered to be by a separatist movement. Almost no other database identified this significant series of attacks.

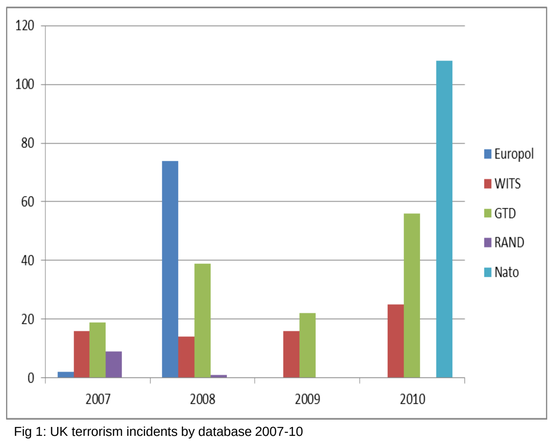

Fig 1: UK terrorism incidents by database 2007-10

	Europol	WITS	GTD	RAND	NATO COE-DAT
Managed	Law Enforcement	Government	Academic	Private	Millitary
Codebook	No	No	Yes	No	No
Coverage	European Union	Global	Global	Global	Global
Time	01/01/2007 to present	01/01/2004 to present	1970-present	1968-2009	2010-present
Status	Constant update	Discontinued	Annual	Dormant	Annual
Sources	Government	Open/Government	Open/Private	Open	Open
Attack Types	0	17	9	10	13
Target Types	0	36	22	17	0
Incident criteria	3	36	15	19	0
Definitions	Group type only	No	Yes	No	No
Non-attacks	Yes, and arrests	No	No	Yes	Yes
UK attacks 2007-20010	76	73	62-136	10	108
Total incidents	2532	Circa 90,000	104,689	40,129	29,753

Fig 2: Table of database attributes

Forecasting results

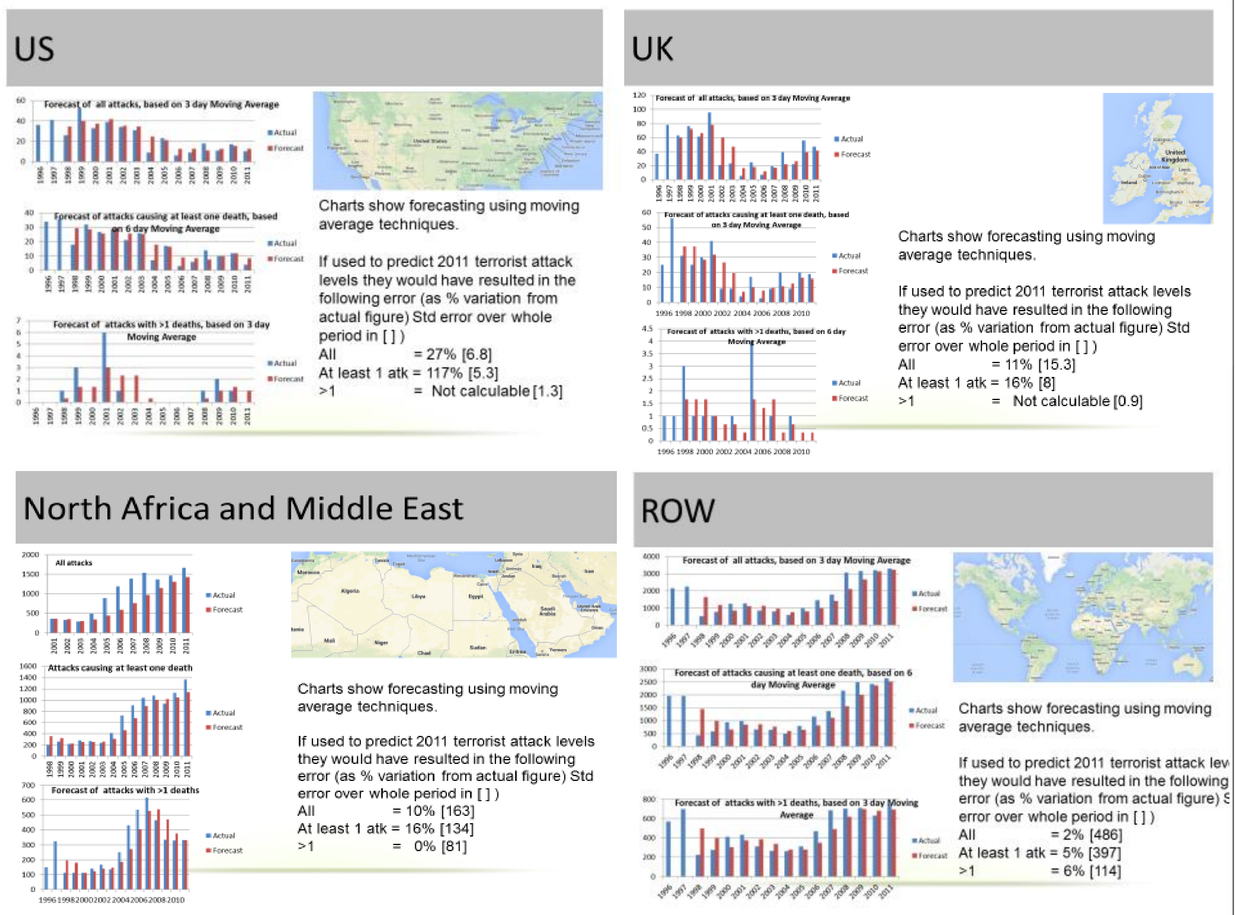

Fig 3: Summarised results of forecasting by region, for all attacks, attacks with 1 death, and more than 1 death

Analysis

As the techniques used are quite blunt trend following methods, and the resolution of sample data for this pilot quite large and heterogeneous it was note expected to yield good results. However when looks at attacks that killed more than 1 person demonstrated some interesting results for the accuracy of a single year prediction. While any level of inaccuracy may feel unsuitable for security policy decisions it appears that there may be potential for further exploration for policy and insurance forecasting purposes with acceptable levels of (in)accuracy.

Further research

Defining terrorism frequency

The most immediate problem of any database that attempts to capture and record instances of terrorist activity is to define what a 'terrorist incident' or 'terrorist attack' actually means. There exists no internationally recognised term, but there have been many attempts to generate definitions. As presented in the literature review it is suggested to use the UK legal tests from the 2000 Terrorism Act. This fulfils the initial objective of creating a database which is appropriate for UK terrorism modelling and is flexible enough to allow the incorporation of other definitions.

Any multi-territorial database will automatically run in to the problem of whether to define the inclusion of an incident by its own countries definition or by the attacked countries definition. A prime example of this is that the Japanese did not consider Aum Shrinryko to be a terrorist group but an extremist religious group. The US, and others, refer to the groups attacks as terrorism though, due to their own definitions. Sometimes these definitions are by exclusion. I.e. Aum's attacks weren't war, nor were they simply crime, therefore they were terrorism. So in any analysis of historical data it makes more sense to begin the analysis on a country by country basis in order not to confuse definitions.

The next problem comes in the definition of an attack or incident itself. Some databases include only 'successful' attacks, i.e. an attack which is delivered to the target although it may not function as well as hoped. Others may include plots, threats and hoaxes but in the first two instances these are often the hindsight reporting of evidence coming out in court and can be years old. The Rajneeshee use of pathogens to contaminate salad bars in the US, and other plots, were only discovered years after when they came out as part of another court case. All this information can be indicative of group intentions to carry out attacks, and which type of attacks and targets they might choose so recording it in a useful manner which can be compared with data in other cases is vital.

Defining Attack types

The study showed large variance in the number of attack types within the databases. This is further complicated with the inclusion of more specific details about the weapons used within an attack. A newly constructed database will need to ensure appropriate selection of attack types. A good starting position would be to base attack types on previous DHS analysis (DHS National Planning Scenarios, 2006) and FEMA guidance manuals (FEMA, 2010), combined with analysis of the history of incidents and plots (UK Cabinet Office, 2009). The DHS planning scenarios in particularly describe potential terrorist attack types based on a combination of open source information and intelligence. This can further be compared against expert elicitation and scenario analysis by Gary Ackerman (Ackerman, 2009) and John Tucker of MIT (Tucker, 2000). Combining these sources of information on attack types with the attack types included within the databases can generate a better structure related to the effective impact of the attack.

Defining Target Types

There is an established government principle in generating lists of threatened targets which are often grouped by type. This is in use by the US (Moteff, The National Asset Database, 2007) and the UK (UK Cabinet Office, 2010) (HMG, 2009). It is only meaningful to have separate categories for targets if there is a shared characteristic within that group that is distinct from another group.

Conclusion

Hypothesis 1 and 2 were disproved although only partially. The quality of terrorism databases could and should be improved and needs to be targeted for a specific purpose. Collection as a general academic activity has led to the datasets being sub-optimal in supporting aspects of forecasting without significant enrichment and transformation.

Ackerman, G., & Tamsett, J. (2009). *Jihadists and Weapons of Mass Destruction.* CRC Press.
FEMA. (2010). FEMA 452 Risk assessment for mitigating a terrorist attack. FEMA.
FEMA. (2010). FEMA 426 Reference Manual to mitagate potential terrorist attacks against buildings. FEMA.
Moteff, J. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and managing threats, vulnerabilities and consequences. Washington: Congressional Research Service.
Moteff, J. (2007). The National Asset Database. Washington: CRS.
Tucker, J. (2000). Toxic Terror: Assessing Terrorist use of chemical and biological weapons. Cambridge, MA: MIT Press.
UK Cabinet Office. (2009). UK National Risk Register 2009. London: HMG.
UK Cabinet Office. (2010). National Risk Register 2010. London: HMG

www.cranfield.ac.uk

S.Johnson@cranfield.ac.uk
Cranfield Forensic Institute, Cranfield University,Defence Academy of the United Kingdom
Shrivenham, Swindon SN6 8LA, UK